AN INVESTIGATION INTO ACCESS CONTROL FOR MOBILE DEVICES

Stephen Perelson[1] and Reinhardt Botha[2]

[1,2]Department of Business Information Systems, Port Elizabeth Technikon, South Africa

[1]stephen@petech.ac.za, +27 41 5043315, Private Bag X6011, Port Elizabeth, 6000
[2]rbotha@computer.org, +27 41 5043669, Private Bag X6011, Port Elizabeth, 6000

ABSTRACT

Mobile devices, such as mobile phones, are becoming multi-purpose devices. These devices are capable of storing data as well as running custom applications. As more people adopt these devices and begin to use them for personal or business tasks, the need for controlling access to the data stored within the device will become vital. This paper presents an investigation of the current trends and techniques being used for access control on mobile devices. It will identify the features that the various embedded operating systems and current mobile applications employ for access control. This investigation also identifies some of the gaps that are apparent in the implementation of these access controls. The aim of this investigation is to motivate further research into a standard access control framework that will engender trust in users of mobile devices. Such a framework should also allow for corporate access control policies to extend onto the mobile device, thereby gaining the trust of the business.

KEYWORDS

Access Control, Security, Mobile Devices

AN INVESTIGATION INTO ACCESS CONTROL FOR MOBILE DEVICES

1 INTRODUCTION

For the purposes of this paper a mobile device is any small, hand-held electronic data processing device. This definition thus includes mobile phones and personal digital assistants but does not include larger devices such as notebook computers. These smaller devices are continuously being improved upon in the areas of performance and storage capacity, not to mention features. These improvements enable mobile devices to run a diverse collection of applications and, as such, facilitate adoption by mobile workers [1, 2].

Users of these mobile devices expect to be able to use them to communicate, manage tasks and contacts, read email, run custom applications, and connect to remote information repositories. The convergence of mobile devices into multi-purpose offerings is helping to fuel the demand for these devices and of the associated service and software offerings. Additionally, as the market matures, users will begin to identify the advantages of needing only one device when they are away from the office [3].

There are advantages to businesses as well, as they will only need to buy a relatively cheap mobile device for each mobile user. The idea of buying a device that can essentially do what a more expensive notebook computer and mobile phone does is a very attractive option. However, the cost of the hardware is not the only expense a business should be aware of. One such expense is the value associated with lost or stolen data [4].

While losing a cheap mobile device may not seem like much of a problem to a business, the risk of losing corporate data should not be taken lightly. A corollary can be drawn between the risk and cost involved with the loss of a notebook computer and the risk associated with the loss of a mobile device [4]. This risk is borne from the increased data storage evidenced in mobile devices allowing more business data to be stored. As more business data is stored on the mobile device, the risk associated with the loss of the mobile device increase. One way to reduce this risk is to employ security mechanisms [5], which can then be used to enforce a business' security policies for mobile workers.

Access control, a security service, can help enforce the business' security policies for mobile workers. However, this requires that the mobile device has sufficient access control mechanisms in place to secure any stored data and functionality [6]. Access control mechanisms are being built into many devices. Many high-end mobile devices have biometric controls as well as the more mainstream password systems. However, from a business perspective, it is important to have standards in place that will inform the business user that a particular mobile device meets a certain level of security with regards to access control [7]. Unfortunately, there seems to be no widely adopted standard for access control services in mobile devices, and there seems to be no consensus over standard access control routines in the various mobile device operating systems. It seems as though data security on mobile devices does not have a high priority. Manufacturers have spent most of their efforts designing security routines for the communication protocols rather than for the data and applications stored on mobile devices. Despite these efforts, research conducted by the Gartner Group indicates that up to 90% of mobile devices have inadequate security [8].

This paper will thus focus on an investigation of the current methods employed by mobile devices to control access to the data stored on the device. It will thus motivate further research into a generic access control framework for mobile devices to ensure trust in users and adherence to corporate access control policies. In order to assess the access control services offered by the mobile device operating systems it is necessary to understand what access control actually entails. After which, an investigation into the access control services offered by the major mobile operating systems will be reviewed and then discussed.

2 ACCESS CONTROL

A business should be able to specify who can access information. Not only would they specify how and when it can be accessed, but also under which conditions [9]. As such, access control is seen as an indispensable part of any information sharing system [10]. There is no doubt that mobile devices form part of an information sharing system.

Access control forms part of five security services, the other four services are: authentication, confidentiality, integrity and non-repudiation [11].

- Authentication service – provides services to confirm the claimed identity.
- Confidentiality service – ensures that information is not erroneously disclosed.
- Integrity service – ensures that the information being accessed is not corrupted in any way.
- Non-repudiation service – ensures that the information received is from the correct source.
- Access control service – synonymous with authorisation, controls the rights granted to authorised users.

These security services are interdependent. The access control service, for example, relies on the user being properly authenticated by the authentication service. Also, the access control service can maintain confidentiality as it will restrict information access to only those users that are authorised. As such, when investigating the access control services on a mobile device it is necessary to take into account any of the five security services that are available as any of them may be used to enforce access control.

Access control on mobile devices can be implemented with a combination of these security services and features. Primarily, these security services are authentication and authorisation. To a lesser degree are the other three security services. These security services and features are shown in table 1.

Table 1: Security services and related features for access control

Authentication	**Authorisation**	**Other**
Passwords	File masking	Encryption
Biometrics	Access Control Lists	Synchronisation
Auto Logout	Role-Based Access Control	

Features that are classified under Authentication include:

- Passwords – A private value known only by authorised users in order to authenticate them. Is synonymous with the concept of a security pin.
- Biometrics – A hardware based solution that examines a physical attribute of an authorised user in order to authenticate them.
- Auto Logout – The device logs the user out after a set time limit. This typically involves turning off to conserve energy.

Features that are classified under Authorisation include:

- File Masking – The system prevents certain protected records from being viewed without the user authenticating themselves.
- Access Control Lists – Permissions for a particular object are associated with users in the form of a matrix [12].
- Role-Based Access Control – Permissions are associated with roles and users get associated with roles. Users thereby receive the permissions based on the roles they are assigned [13].

Features that are classified under Other include:

- Encryption – Mechanisms to encrypt data that could include public key routines. Part of the confidentiality service.
- Synchronisation – Allows for the backing up and restoration of data and settings of a particular mobile device.

Not all of these features are available on all mobile devices. The one that is always present is the password control, but biometric controls, such as fingerprint readers, are becoming more common. Access control on a mobile device typically involves an activation challenge based on a password or biometric measure [14]. Full access is then granted to all data and applications once the device is activated with the correct password. This process, depicted in figure 1, involves confirming the user's identity (authentication) and, based on that confirmed identity, allow access to a resource (authorisation).

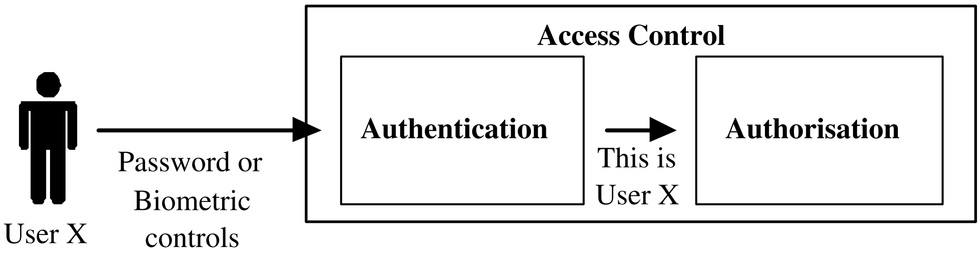

Figure 1: The process flow towards access control on mobile devices

Since a mobile device is typically a personal device, the need to authorise a user is not considered important as the authentication process infers that the user is authorised. It is also assumed that all the data stored on the device is owned by the person using it. This assumption causes problems when the user is a mobile worker and data is owned by the corporation. Corporate environments are extending beyond the boundaries of the office block. Yet, it is still important for a business to be able to enforce their corporate access control policies on mobile workers, wherever they may be. Hence, the corporate access control policies need to be extended to the mobile device. To understand how this can be achieved, it was necessary to investigate the current access control services and features available on mobile devices.

Another reason for this investigation is to understand how access control could be standardised to ensure a high level of trust in mobile devices. This investigation had to take into account what access control features are available through the different operating systems. The purpose of the investigation was to gain an understanding of the area of research and to identify the feasibility of conducting further research into this area. The next section provides a description of the investigation and a brief outline of the results of the investigation.

3 THE INVESTIGATION

This investigation took into account what access control features are available through the different mobile device operating systems. It was important that the investigative technique employed allowed the current trends with regards to access control services in mobile devices to be understood. The investigation did not take into account 3rd party security utilities, nor did it take into account possible extensions to the operating system introduced by a particular manufacturer.

3.1 The Investigative Technique

The investigative technique entailed researching the documentation for each of the major mobile device operating systems, for which interested readers may visit [15, 16, 17, 18]. Where possible, a practical analysis of a mobile device was also conducted. This research sought to identify possible access control routines that could be used to control access to locally stored data. It also sought to identify routines that could be used by applications running on a mobile device to control their access requirements. It was also necessary to identify routines in other runtime environments such as the Java runtime and the .NET compact framework.

These routines usually form part of other security services. The most notable of these security services is authorisation, which is synonymous with access control. As such, it was thus necessary to identify these security mechanisms in the mobile device operating systems. It was also necessary to identify future access control trends in order to judge how the mobile device operating systems are going to change to handle access control services in the future.

3.2 The Investigation Domain

Various mobile device operating systems were identified. These included: Microsoft's Pocket PC and Smartphone operating systems with the .NET compact framework; Symbian OS 8; and Palm OS 5. While Linux is becoming more popular it was decided not to investigate this operating system, or the Embedded Linux version, as it has yet to be widely adopted by the corporate market.

All of the reviewed operating systems have encryption capabilities that could be used by applications. Unfortunately, few of these operating systems support strong encryption where such encryption involves 128 bit cyphers. In part, this is due to the fact that strong encryption tends to be processor intensive [19]. Applications written for mobile devices are able to make use of these encryption routines as well as any other security services that are built into the host operating system. Developers would have to implement any other security services themselves if those services are not available. Not having a standardised security architecture hinders the creation of secure software that can be ported easily to the different mobile device operating systems.

The Symbian operating system, having grown from the EPOC operating system, has become the operating system of choice for many of the mobile phone manufacturers such as Nokia and Siemens. It is being used in many products that combine personal digital assistant (PDA) type functionality with cellular phone features. Palm OS is probably wider known due to the popularity of the Palm personal digital assistant. Palm OS was extended to handle cellular communication in a few Palm models but functions primarily as a PDA. Microsoft's Pocket PC operating system is part of Microsoft's embedded operating systems family [20]. The Pocket PC operating system seems to require relatively higher hardware specifications than the other operating systems. The reason is not that the operating system is power hungry, but rather that Microsoft have identified the need for the power and storage requirements to run the applications users expect. Microsoft have identified the need for a similar operating system for mobile phones and have designed their Smartphone operating system. The Smartphone OS has most of the features found in the Pocket PC OS.

3.3 The Investigation Findings

What follows is a short description of the main mobile device operating systems.

3.3.1 Pocket PC and the Smartphone OS

Both the Pocket PC 2003 OS and the Smartphone 2003 OS form part of the Windows Mobile 2003 collection of operating systems and are therefore expected to have similar features and capabilities. The Windows Mobile 2003 collection is based upon Microsoft's Windows CE .NET 4.2, an operating system with a componentised architecture to allow for its adoption into a wide variety of devices [21]. While the feature set for the Pocket PC OS and Smartphone OS is relatively consistent it is very likely that a manufacturer will implement unique hardware features with the associated device drivers [22]. Such features may include smartcard readers or biometric password controls, which would then form part of the access control of the device.

As such, these operating systems support physical access control, which is part of the perimeter security of the device. Physical access control takes into account unlocking of the device through a password or biometric measure. It also supports automatic device locking after a time-out period. As already mentioned, the authentication provided for by the password based locking mechanism infers the authorisation of the user. The device's synchronisation mechanism is also locked when the device lock is activated and every failed unlock attempt causes an exponential delay to be incurred thereby preventing automated brute-force attacks on the synchronisation mechanism [23].

Roles form part of the security of this operating system but they do not mirror an organisation's roles. These roles get used when dealing with communications and when handling executable code. Included as part of the latest Pocket PC and Smartphone operating systems is the .NET compact framework. The .NET compact framework allows for code-based security where code can be signed and given the rights to access protected services [24].

3.3.2 Symbian OS

Symbian OS, currently at version 8, is also a modular operating system with many features that a manufacturer could implement [25]. For security, Symbian OS does offer security certificates and cryptography that enable it to manage code and communication security [26]. It does have the expected password protection of the device as well as password services and encryption routines that application developers can use [25]. Version 8 also offers a digital rights management system that caters for executable program files as well as media files [25].

3.3.3 Palm OS

The Palm operating system is also modular, thereby allowing application developers to extend the security of the device. Even though 3rd party security applications are not being examined in this investigation, it should be mentioned that many security applications take advantage of this modular design [27]. Palm OS provides password-based user authentication with automatic device locking and also allows records to be hidden or masked thereby protecting sensitive data [27, 28]. Future plans for Palm OS include system-wide access control, which will take the form of access control for databases, individual resources, and other objects [28].

3.3.4 Java 2 Platform, Micro Edition

Java applications are restricted to the access control routines available in the version of the Java runtime environment installed on the mobile device. In the case of mobile devices, the version of the Java runtime that is usually available is the Java 2 Platform, Micro Edition (J2ME). To enable Java applets on the smaller mobile devices, a specialised architecture and set of application programming interfaces for J2ME was designed and is known as the Mobile Information Device Profile (MIDP) [29].

MIDP applets, or midlets, have a complex security framework to ensure code security. Midlets rely on the mobile device to ensure that the correct access rights are granted. These access rights may include being able to access data on the device if the midlet was trusted [29].

Overall, the security features of MIDP is very limited. The reason behind this decision was the need to address only those areas that were considered indispensable in order to achieve portability [29].

4 DISCUSSION

All of the mobile device operating systems have certain similar features. These features include a modular design and basic security services such as authentication and encryption. A modular design enables manufacturers of mobile devices to pick and choose the features of the operating system they want to implement. Basic authentication attempts to authenticate the user attempting to access the device. Once the user is authenticated they are assumed to be authorised to access all resources and data stored on the device. Encryption services normally get used for communication but these services could be utilised by applications to encrypt data. These are not the only features of the mobile device operating systems.

Some of the operating systems have a feature known as code access security, which attempts to prevent untrusted code from getting access to resources that could be detrimental to the integrity of the mobile device. This feature resembles access control, however, it only concerns installed applications and downloaded code. This feature does not help enforce corporate access control policies. Also, some of the features listed in table 1 are not found in the mobile device operating systems. These feature are role-based access control that mimics the organisation's roles and access control lists. The features listed in table 1 are reproduced in table 2 showing the availability of each feature in each of the investigated mobile device operating systems.

Table 2: Availability of security features

	Pocket PC & Smartphone	**Symbian OS**	**Palm OS**	**J2ME**
Passwords	✔	✔	✔	✘
Biometrics	✔	✘	✔	✘
Auto Logout	✔	✔	✔	✘
File Masking	✘	✘	✔	✘
Access Control Lists	✘	✘	✘	✘
Role-Based Access Control	✔	✘	✘	✘
Encryption	✔	✔	✔	✔
Synchronisation	✔	✔	✔	✘

Some points about the summary displayed in table 2 include:

- Any application can be written to incorporate these features but this investigation was restricted to the features available in the operating systems and the J2ME runtime.
- J2ME is a runtime environment that relies heavily upon the host operating system for certain services. As such, many of the listed features are not handled by the runtime.
- Role-based access control is a feature of the Pocket PC and Smartphone operating systems, but this feature does not resemble an organisation's roles. Rather, it deals with code-access security.
- Encryption is supported to some degree on all operating systems. This is usually required for communication.
- There are large gaps in the features of the authorisation service.

Although all of the evaluated mobile device operating systems have basic authentication services in place, these are not enough to enforce corporate access control policies. Corporate access control policies seek to prevent unauthorised access to corporate data or resources that may be stored on a mobile device. As can be seen in table 2, there are noticeable gaps in the authorisation capabilities of all of the investigated operating systems. These capabilities include role-based access control and access control lists. The reason behind this rationale is that a mobile device is considered to be a personal device and, as such, does not contain corporate data or resources. However, mobile devices are being adopted for use in the corporate environment. As such, corporate access control policies need to be extended onto this platform. None of the mobile device operating systems that were investigated support this demand.

Future developments may bring access control services into these operating systems. However, since these operating systems are modular in design, a manufacturer may not implement some or all of the access control services for a variety of reasons. A standardised access control architecture would help manufacturers choose the best access control services for a particular mobile device. This would thus engender trust in the access control capabilities of the device and promote the adoption of these mobile devices into the corporate arena. Also, standards are important as a promoter of trust as can be evidenced by the Trusted Computer Evaluation Criteria (TCSEC) [7].

This access control architecture would have to be flexible to cater for the requirements of any corporate access control policies that may need enforcing. Not having a standardised framework for access control routines on mobile devices may prevent businesses from sanctioning the use of these devices for conducting business.

5 CONCLUSION

This investigation aimed to gain an understanding of the access control services that mobile device operating systems provide. The results of this investigation show that current mobile devices cannot enforce corporate access control policies. This requirement is becoming more important as these devices are entering the corporate environment. Identifying this need for access control services within mobile devices allows further research to be conducted. Further research will thus be conducted to ascertain what the access control requirements are for mobile devices. These requirements will need to take corporate access control policies into account. The eventual aim is to create a generic access control framework that will be able to enforce corporate access control policies and, as such, will engender trust in mobile devices by all parties.

Towards this aim, another concept for future research is that of packaged access rights. This entails storing the access rights for a particular document together with that document. This concept is currently being used in many digital rights management (DRM) implementations. It may be possible to use this approach to control corporate access control policies in a mobile environment. However, before a solution can be discovered it will be necessary to formalise the concept of corporate access control. This is necessary in order to understand the requirements for extending corporate access control into the mobile environment. At the same time, it will be necessary to evaluate the user's perspective with regards to mobile work and security requirements. This is important in order to understand the user requirements with respect to corporate access control for mobile devices.

6 ACKNOWLEDGEMENTS

All trademarks and copyrights are the property of their respective owners. The financial assistance of the National Research Foundation (NRF) towards this research is hereby acknowledged. Opinion expressed and conclusions arrived at, are those of the authors and are not necessarily to be attributed to the National Research Foundation.

7 REFERENCES

[1] Canalys. Smart phones will overtake handhelds this year in emea [online]. 2003 [cited 20 April 2004]. Available from: `http://www.canalys.com/pr/2003/r2003031.htm`.

[2] Legand L. Burge, III, Suleiman Baajun, and Moses Garuba. A ubiquitous stable storage for mobile computing devices. In *Proceedings of the 2001 ACM symposium on Applied computing*, pages 401–404. ACM Press, 2001.

[3] Carl Zetie. Convergence or divergence: What's next for mobile devices? [online]. 2004 [cited 20 April 2004]. Available from: `http://www.informationweek.com/story/showArticle.jhtml?articleID=18311545`.

[4] Robert Richardson. 2003 CSI/FBI computer crime and security survey. Computer Security Institute, 2003. Available from: `http://www.gocsi.com/forms/fbi/pdf.jhtml`.

[5] Rossouw von Solms. Information security management (3): the code of practice for information security management (BS 7799). *Information Management & Computer Security*, 06(5):224–225, 1998.

[6] Anup K. Ghosh and Tara M. Swaminatha. Software security and privacy risks in mobile e-commerce. *Commun. ACM*, 44(2):51–57, 2001.

[7] R. von Solms. Information security management: Why standards are important. *Information Management and Computer Security*, 7(1):50–57, 1999.

[8] Steve Gold. Ninety per cent of mobile devices have no IT security [online]. 2004 [cited 20 April 2004]. Available from: `http://www.securesynergy.com/securitynews/newsitems/2004/apr-04/020404-08.htm`.

[9] R. S. Sandhu, E. J. Coyne, H. L. Fenstein, and C. E. Youman. Role-based access control models. *IEEE Computer*, 29(2):38–47, Feb 1996.

[10] HongHai Shen and Prasun Dewan. Access control for collaborative environments. In *Proceedings of the 1992 ACM conference on Computer-supported cooperative work*, pages 51–58. ACM Press, 1992.

[11] ISO 7498-2: Information Processing Systems — Open System Interconnection — Basic Reference Model – Part 2: Security Architecture, 1989.

[12] John Barkley. Comparing simple role based access control models and access control lists. In *Proceedings of the second ACM workshop on Role-based access control*, pages 127–132. ACM Press, 1997.

[13] R. S. Sandhu. Role-based access control. *Advances in Computers*, 46:9–19, 1998.

[14] Jian Tang, Vagan Terziyan, and Jari Veijalainen. Distributed pin verification scheme for improving security of mobile devices. *Mob. Netw. Appl.*, 8(2):159–175, 2003.

[15] Microsoft. Mobile and embedded development [online]. 2004 [cited 10 June 2004]. Available from: `http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnanchor/html/mobileembedded.asp`.

[16] PalmSource. Palm Software and Palm OS [online]. 2004 [cited 10 June 2004]. Available from: `http://www.palmsource.com`.

[17] Symbian. Symbian OS [online]. 2004 [cited 10 June 2004]. Available from: http://www.symbian.com/.

[18] Sun Microsystems. Java 2 Platform, Micro Edition (J2ME) [online]. 2004 [cited 10 June 2004]. Available from: http://java.sun.com/j2me/index.jsp.

[19] Microsoft. Cryptographic support for the pocket PC [online]. October 2003 [cited 22 April 2004]. Available from: http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnsmtphn2k3/html/smartphone_security.asp.

[20] Microsoft. Windows embedded family overview [online]. 2004 [cited 10 June 2004]. Available from: http://msdn.microsoft.com/embedded/prodinfo/prodoverview/family/default.aspx.

[21] Microsoft. Comparison of Windows CE .NET 4.2, Pocket PC 2002, and Windows Mobile 2003 Software for Pocket PCs, 2003. Available from: http://go.microsoft.com/fwlink/?LinkId=19383 [cited 11 June 2004].

[22] Microsoft. Drivers [online]. 2004 [cited 11 June 2004]. Available from: http://msdn.microsoft.com/embedded/ce.net/drivers/default.aspx.

[23] Microsoft. Pocket PC adaptation kit for mobile operators - device lock [online]. October 2003 [cited 22 April 2004]. Available from: http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnsmtphn2k3/html/smartphone_security.asp.

[24] James Pratt. A practical guide to the smartphone application security and code signing model for developers [online]. February 2003 [cited 22 April 2004]. Available from: http://msdn.microsoft.com/security/default.aspx?pull=/library/en-us/dnsmtphn2k3/html/smartphone_security.asp.

[25] Sander Siezen. Symbian os version 8.0 functional description [online]. 2004 [cited 11 June 2004]. Available from: http://www.symbian.com/technology/symbos-v8x-det.html.

[26] Symbian. Symbian OS Security Architecture Overview [online]. 2002 [cited 22 April 2004]. Available from: http://www.symbian.com/developer/techlib/v70sdocs/doc_source/DevGuides/SecurityGuide/SecurityArchitectureOverview.html#SAOverview.

[27] PalmSource. Security and Palm OS, 2002. Available from: http://www.palmsource.com/includes/security.pdf [cited 22 April 2004].

[28] Ezekiel Sanborn de Asis. Strategic directions for security on the Palm OS, 2002. Available from: http://www.palmsource.com/jp/palmsource/pdf/slides-2002/106.pdf [cited 22 April 2004].

[29] Sun Microsystems. Mobile Information Device Profile Specification 2.0 Final Release, November 2003. Available from: http://jcp.org/aboutJava/communityprocess/final/jsr118/index.html [cited 22 April 2004].